**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270-

**Deliberate threats**

1. When does intentional damage occur?

Intentional damage occurs when an individual or grop deliberately sets out to cause problems within a information system whether the aim is the hardware, software or data ect.

1. Unauthorised access is both physical and logical. Explain what this means?

Unauthorised access may be either/both physical and logical as it can be defined as to use a reasource without permission hence it may include; intruders physically or via a electronic connection method, those accessing a file or computer without permission ect.

1. Computer Virus
   1. Describe the nature of this virus.

A computer virus infects in much the same way that a biological would hence the name. they may be one of many types for a specific purpose.

* 1. What is the main purpose of a virus?

The main purpose of a virus is to affect the running of a computer in a manner unintended by its user by releasing a payload.

* 1. What is meant by the term, payload?

The payload or warhead is the action that the virus is designed to carry out whether it be deleting files (vital or not), slowing performance or other malicious deeds. It is worth noting that all viruses are intentionally dangerous with some simply protesting for a cause.

* 1. Describe a worm?

A worm is a virus that self-replicates to take up space on a hard disk on a single workstation or server. Many virus can fall into this category by using or definition.

* 1. List the other types of viruses, p 272, fig. 7-10.
* Boot infectors that attack the critical section of a hard drive, launching on boot the malicious code is run by the system and then spread from within the OS making the computer vulnerable to intruders
* Executables ie when a executable file (.vbs, .exe, .bat, .com, .sys, .dll, .reg ect) is infected by a virus (may infect boot)
* Macro viruses are common to computers running MS office applications due to the inbuild Visual basics engine allowing for sophisticated macros relatively easy. It may prevent files from saving or delete, alter data, open other programs or alter Mail settings ect.
* A time bomb is an action/virus that can be triggered by a predefined time or date ‘event’ occurring, another similar varieant is the logic bomb.
* A logic bomb triggers a action in response to a event or condition being met.
* Worm is mentioned above in prior question.
* Trojan horse is when a viruses payload is hidden behind a seemingly normal item ie programs that are offered for free will often have one.
* A resident virus installes its self into the memory of a computer by infecting files and programs already installed. It finds a method to allocate memory to itself and then replicate.
* Polymorphic are viruses that encrypt themselves in a different way each time of infection making antivirus programs often falter to protect.
  1. How do viruses mainly spread?

Viruses mainly spread by email attachments however use of removable media (sometime even just the simple act of plugging it in) are antoher typical method. Less common however still one of the many possibilities include opening a infected file on a network.

1. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?

A hacker is a person who gains unauthorised access through logical means for a look at the data or challenge as such they aren’t considered as bad as a cracker will proceed to damage, alter, destroy or steal the data.

1. Tampering with files
   1. Describe how employees tamper with files.

Employees generally tamper with files because they were given unrestricted access to files that they shouldn’t need access too. Similarly employees may tamper by applying methods of a cracker due to a dispute, industrial sa ect.

* 1. What is industrial sabotage?

Industrial sabotage is when a hacker or cracker applies their methods for benefits to their own ‘company’ ie affecting the stock prices ect.

1. Information theft
   1. Why does this occur?

Information theft occurs because some less scupelus businesses wish to have the edge without any of the main work, similarly they may find something they could shut the business down for ect.

1. Vandalism of hardware

Vandalism of hardware is when hardware is broken to deliberately damage it. Commonly it may include; cutting, snapping, bending, introducing foreign matter ect.

1. Theft of hardware

Theft of hardware occurs due its high demand/ transferability. Many items of technology are similarly worth something hence may be stolen for selling or simply to mean that they don’t have to pay for it. Common items include laptops, ram, hard disks, CD’s and DVD’s ect.

**Accidental threats**

1. User error
   1. List some common examples of user error.

Common examples of user error include;

* Inproper use due to not understanding what doing ie changing a setting, not saving a file with proper extention ect.
* Saving over a file or not naming it using file conventions
* Deleting without thinking
* Preforming irreversible steps such as formatting when it shouldn’t of happened
* Not closing files properly or force shutting down
* Ignoring prompts
  1. What processes are in place to limit user error.

Event driven dialogue message boxes to confirm a action is intended.

1. Failure to follow file-management procedures
   1. List common errors of employees in saving files.

* File extensions incorrect or left of completely
* Non descriptive file names
* Folders improperly used

**Technical Failure**

1. List some examples of technical failure.

* Non essential failure/ easy fixes such as peripherals
* Non critical failure (still put the device out of service) ie graphic card ect
* Critical failure ie disk drive, fire damage ect (ones you hope you have a backup)

The above may occur thorugh accidental breakage, age or unknown

**Consequences of violating security and privacy measures, p 278**

1. List three important consequences if security measures are violated.

Breach of privacy

Loss of property

Loss of income due to inaccessibility